

Introduced by Senator Machado

February 23, 2006

An act to amend and repeal Section 1798.82 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 1512, as introduced, Machado. Privacy: personal information: security.

Existing law requires any person or business conducting business in California that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law permits substitute notice of the breach to be provided if the person or business demonstrates that the cost of providing notice would exceed \$250,000.

This bill would change the threshold for providing substitute notice from \$250,000 to \$500,000. The bill would also repeal duplicative provisions of law.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. Section 1798.82 of the Civil Code, as added by
- 2 Section 4 of Chapter 1054 of the Statutes of 2002, is amended to
- 3 read:
- 4 1798.82. (a) Any person or business that conducts business
- 5 in California, and that owns or licenses computerized data that

1 includes personal information, shall disclose any breach of the
2 security of the system following discovery or notification of the
3 breach in the security of the data to any resident of California
4 whose unencrypted personal information was, or is reasonably
5 believed to have been, acquired by an unauthorized person. The
6 disclosure shall be made in the most expedient time possible and
7 without unreasonable delay, consistent with the legitimate needs
8 of law enforcement, as provided in subdivision (c), or any
9 measures necessary to determine the scope of the breach and
10 restore the reasonable integrity of the data system.

11 (b) Any person or business that maintains computerized data
12 that includes personal information that the person or business
13 does not own shall notify the owner or licensee of the
14 information of any breach of the security of the data immediately
15 following discovery, if the personal information was, or is
16 reasonably believed to have been, acquired by an unauthorized
17 person.

18 (c) The notification required by this section may be delayed if
19 a law enforcement agency determines that the notification will
20 impede a criminal investigation. The notification required by this
21 section shall be made after the law enforcement agency
22 determines that it will not compromise the investigation.

23 (d) For purposes of this section, “breach of the security of the
24 system” means unauthorized acquisition of computerized data
25 that compromises the security, confidentiality, or integrity of
26 personal information maintained by the person or business. Good
27 faith acquisition of personal information by an employee or agent
28 of the person or business for the purposes of the person or
29 business is not a breach of the security of the system, provided
30 that the personal information is not used or subject to further
31 unauthorized disclosure.

32 (e) For purposes of this section, “personal information” means
33 an individual’s first name or first initial and last name in
34 combination with any one or more of the following data
35 elements, when either the name or the data elements are not
36 encrypted:

37 (1) Social security number.

38 (2) Driver’s license number or California Identification Card
39 number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed ~~two hundred fifty~~ *five hundred* thousand dollars ~~(\$250,000)~~ *(\$500,000)*, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 915 of the Statutes of 2002, is repealed.

~~1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the~~

1 breach in the security of the data to any resident of California
2 whose unencrypted personal information was, or is reasonably
3 believed to have been, acquired by an unauthorized person. The
4 disclosure shall be made in the most expedient time possible and
5 without unreasonable delay, consistent with the legitimate needs
6 of law enforcement, as provided in subdivision (c), or any
7 measures necessary to determine the scope of the breach and
8 restore the reasonable integrity of the data system.

9 (b) Any person or business that maintains computerized data
10 that includes personal information that the person or business
11 does not own shall notify the owner or licensee of the
12 information of any breach of the security of the data immediately
13 following discovery, if the personal information was, or is
14 reasonably believed to have been, acquired by an unauthorized
15 person.

16 (c) The notification required by this section may be delayed if
17 a law enforcement agency determines that the notification will
18 impede a criminal investigation. The notification required by this
19 section shall be made after the law enforcement agency
20 determines that it will not compromise the investigation.

21 (d) For purposes of this section, “breach of the security of the
22 system” means unauthorized acquisition of computerized data
23 that compromises the security, confidentiality, or integrity of
24 personal information maintained by the person or business. Good
25 faith acquisition of personal information by an employee or agent
26 of the person or business for the purposes of the person or
27 business is not a breach of the security of the system, provided
28 that the personal information is not used or subject to further
29 unauthorized disclosure.

30 (e) For purposes of this section, “personal information” means
31 an individual’s first name or first initial and last name in
32 combination with any one or more of the following data
33 elements, when either the name or the data elements are not
34 encrypted:

35 (1) Social security number.

36 (2) Driver’s license number or California Identification Card
37 number.

38 (3) Account number, credit or debit card number, in
39 combination with any required security code, access code, or

1 ~~password that would permit access to an individual's financial~~
2 ~~account.~~

3 ~~(f) For purposes of this section, "personal information" does~~
4 ~~not include publicly available information that is lawfully made~~
5 ~~available to the general public from federal, state, or local~~
6 ~~government records.~~

7 ~~(g) For purposes of this section, "notice" may be provided by~~
8 ~~one of the following methods:~~

9 ~~(1) Written notice.~~

10 ~~(2) Electronic notice, if the notice provided is consistent with~~
11 ~~the provisions regarding electronic records and signatures set~~
12 ~~forth in Section 7001 of Title 15 of the United States Code.~~

13 ~~(3) Substitute notice, if the person or business demonstrates~~
14 ~~that the cost of providing notice would exceed two hundred fifty~~
15 ~~thousand dollars (\$250,000), or that the affected class of subject~~
16 ~~persons to be notified exceeds 500,000, or the person or business~~
17 ~~does not have sufficient contact information. Substitute notice~~
18 ~~shall consist of all of the following:~~

19 ~~(A) E-mail notice when the person or business has an e-mail~~
20 ~~address for the subject persons.~~

21 ~~(B) Conspicuous posting of the notice on the Web site page of~~
22 ~~the person or business, if the person or business maintains one.~~

23 ~~(C) Notification to major statewide media.~~

24 ~~(h) Notwithstanding subdivision (g), a person or business that~~
25 ~~maintains its own notification procedures as part of an~~
26 ~~information security policy for the treatment of personal~~
27 ~~information and is otherwise consistent with the timing~~
28 ~~requirements of this part, shall be deemed to be in compliance~~
29 ~~with the notification requirements of this section if the person or~~
30 ~~business notifies subject persons in accordance with its policies~~
31 ~~in the event of a breach of security of the system.~~